Release Notes

LCOS LX

6.20 RU1

Inhaltsübersicht

1. Einleitung

Alle Mitglieder der LANCOM Betriebssystem-Familie – LCOS, LCOS SX, LCOS LX und LCOS FX – sind die vertrauenswürdige Grundlage für das gesamte LANCOM Produktportfolio. Im Rahmen der von den Produkten vorgegebenen Hardware ist die jeweils aktuelle Firmware-Version für alle LANCOM Produkte verfügbar und wird von LANCOM Systems kostenlos zum Download angeboten.

Dieses Dokument beschreibt die Neuerungen der LCOS LX Software Release 6.20 RU1.

Beachten Sie vor der Durchführung des Firmware-Update unbedingt die Hinweise im Kapitel 7 „Allgemeine Hinweise“ dieses Dokumentes.

Aktuelle Support-Hinweise und sowie Informationen über bekannte Einschränkungen zur aktuellen LCOS LX -Version finden Sie im Support-Bereich unserer Webseite
www.lancom-systems.de/service-support/soforthilfe/aktuelle-support-hinweise

2. Das Release-Tag in der Software-Bezeichnung

Release Candidate (RC)
Ein Release Candidate ist umfangreich von LANCOM getestet und enthält neue Betriebssystem-Features. Er dient als Praxistest und wird deshalb für den Einsatz in Produktivumgebungen nicht empfohlen.

Release-Version (Rel)
Das Release ist umfangreich geprüft und in der Praxis erfolgreich getestet. Es enthält neue Features und Verbesserungen bisheriger LANCOM Betriebssystem-Versionen und wird daher für den Einsatz in Produktivumgebungen empfohlen.

Release Update (RU)
Ein Release Update dient zur nachträglichen Weiterentwicklung einer initialen Release-Version in Produktivumgebungen und enthält Detailverbesserungen, Security Fixes, Bug Fixes und kleinere Features.

Security Update (SU)
Enthält wichtige Security Fixes des jeweiligen LANCOM Betriebssystem-Versionstandes und sichert Ihnen fortlaufend einen sehr hohen Sicherheitsstandard in Ihrer Produktivumgebung.

3. Gerätespezifische Kompatibilität zu LCOS LX

Grundsätzlich werden alle LANCOM Produkte über die gesamte Lebenszeit regelmäßig mit Major Releases bedient, welche neue Features und Bugfixes beinhalten. Auch für Geräte, die keine aktuelle LCOS LX -Version unterstützen, werden in regelmäßigen Abständen LCOS LX Release Updates inklusive Bugfixes und allgemeinen Verbesserungen bereitgestellt. Eine Übersicht über die aktuell unterstützte LCOS LX -Version für Ihr Gerät finden Sie unter www.lancom.de/lifecycle.

4. Hinweise zu LCOS LX

Informationen zu Werkseinstellungen
Geräte, die mit LCOS LX ausgeliefert werden, kontaktieren automatisch die LANCOM Management Cloud (LMC). Diese Funktionalität ermöglicht eine Zero-Touch-Inbetriebnahme neuer Geräte. Falls die LMC nicht verwendet werden soll, kann diese Funktionalität im LANconfig jederzeit unter ‚Management > LMC' deaktiviert werden. Eine spätere Verwendung der LMC ist jederzeit wieder manuell aktivierbar.

5. Bekannte Einschränkungen

→ Lokale Konfigurationsänderungen werden nicht in die LMC übertragen.
→ Das Skripting des Gerätes aus der LMC wird aktuell noch nicht unterstützt, jedoch die Verwendung von Add-Ins.

6. Historie LCOS LX

Um das AP-Modell LANCOM LW-600 auf LCOS LX 6.20 zu aktualisieren, ist zuvor das Einspielen der Migrations-Firmware LCOS LX 6.14 RU2 erforderlich.

Im Rahmen von Sicherheitsverbesserungen wurde die Verhandlung des für die Verschlüsselung der Kommunikation zwischen WLCs und APs verwendete DTLS-Protokoll angepasst. Aus diesem Grund ist für einen WLC-verwalteten Betrieb von APs mit LCOS LX 6.20 mindestens die LCOS-Version 10.80 RU3 auf dem WLC erforderlich.

LCOS LX - Änderungen 6.20.0139 RU1

Neue Features

→ In RADIUS-Accounting-Nachrichten sind nun die Attribute „framed-ip-address“, „framed-ipv6-address“ und „framed-ipv6-prefix“ enthalten.

Korrekturen / Anpassungen

→ Es war möglich, auf das Verzeichnis /assets/ und dessen Unterverzeichnisse zuzugreifen, ohne dass vorher eine Benutzeranmeldung erfolgte.

→ Die IP-Adresse des Cloud-managed Hotspots wurde nur einmalig bei der ersten Verbindung aufgelöst. Nach einem Wechsel der IP-Adresse des Cloud-managed Hotspots konnten die Access Points diesen nicht mehr erreichen, sodass die Hotspot-Funkionalität bis zu einem Neustart der Geräte nicht mehr gegeben war.
Die Auflösung des Cloud-managed Hotspots wird jetzt alle fünf Minuten durchgeführt.

→ Bei Verwendung des Cloud-managed Hotspots mit externem Captive Portal und einem spezifischen Port (z.B. :8443) wurde der Doppelpunkt nicht übernommen. Dies führte dazu, dass das Captive Portal nicht aufgerufen werden konnte.

→ Wenn die zufällige Kanalwahl in jedem Frequenzband aktiviert war, hatte dies zur Folge, dass bei SSIDs, in denen alle drei Bänder verwendet wurden, die 6 GHz-Funkmodule nicht aktiviert wurden.

→ Es konnte bei den Access Points LANCOM LX-6400 und LX-6402 mit den Hardware-Versionen MOD-B00 und MOD-C00 vorkommen, dass das 2,4 GHz Radio auf dem Kanal 5 eine dauerhaft erhöhte Kanallast aufwies.

→ Es konnte bei durch die LMC verwalteten Access Points vorkommen, dass nach einem Rollout, in welchem eine SSID inaktiv geschaltet war, nicht alle SSIDs vom Access Point übernommen wurden. In der Folge wurden auch einige aktiv geschaltete SSIDs nicht ausgestrahlt und konnten somit nicht verwendet werden.

→ Innerhalb eines L2TP-Tunnels wurde bei Paketen mit bestimmten Größen (16-Byte Schritte - 1470 Byte, 1454 Byte usw.) der VLAN-Header nicht entfernt. Da WLAN-Clients Pakete mit VLAN-Header nicht verarbeiten können, führte dies zu einer stark eingeschränkten Kommunikation.

→ Ein per Dynamic VLAN gelerntes VLAN wurde nicht dem L2TP-Interface in der Bridge zugewiesen. Dies führte dazu, dass per L2TP mit Dynamic VLAN angebundene Clients nicht über den L2TP-Tunnel kommunizieren konnten.

→ Empfing der Access Point vom vorgeschalteten Gateway ein ‚ICMP Fragmentation needed' (weil der Client ein zu großes Paket über den L2TP-Tunnel versendete), baute der Access Point den L2TP-Tunnel ab.

→ Die Access Points sendeten ein ‚ICMP Fragmentation needed' nur über die LAN- und WLAN-Schnittstellen, nicht aber über einen L2TP-Tunnel.

→ Bei Übertragung großer Pakete konnte es vorkommen, dass der L2TP-Tunnel abgebaut wurde. In einem L2TP-Trace auf dem Access Point wurde in diesem Fall die Meldung „failed to send packet: Message too large" ausgegeben.

→ Wurden die IP-Parameter statisch vergeben, speicherte der Access Point das hinterlegte Gateway nicht ab. Dadurch konnte der Access Point nicht mehr mit dem Internet kommunizieren (etwa zwecks Zeitabgleich per NTP).

→ Wenn im WLAN-Controller in der Access-Point-Tabelle der Parameter ‚Ant.-Gewinn-Modus' auf ‚Benutzerdefiniert' gesetzt und zusätzlich die Leistungs-Reduktion konfiguriert wurde, übernahm der Access Point diese Einstellungen korrekt.
Wurde der ‚Ant.-Gewinn-Modus' anschließend wieder auf Standard gesetzt und die Leistungs-Reduktion gelöscht, übernahm der Access Point diese Werte allerdings nicht, sodass die vorigen Werte aktiv blieben.

→ In einem TACACS+-Szenario wurde der Spare-Server auch angefragt, wenn der Main-Server verfügbar war, das Login jedoch ablehnte. Der Spare-Server wird jetzt nur angefragt, wenn der Main-Server nicht verfügbar ist.

→ Nach dem Ausrollen eines neuen Zeitplans auf Access Points mit LCOS LX verblieben diese dauerhaft im Testmodus und die Konfiguration konnte nicht geschrieben werden. Dadurch war keine Kommunikation mit den Access Points möglich. In der LMC wurde die Meldung „Überprüfe Erreichbarkeit" (nach dem ersten Rollout-Versuch) oder „Nicht akzeptiert" (bei weiteren Rollout-Versuchen) angezeigt.

→ Der DHCP-Server des LMC-Hotspots auf einem Access Point unterstützt nur IPv4. Fungierte der Access Point als Hotspot-Gateway und wurde diesem ein IPv6-DNS-Server zugewiesen, verwarf der DHCP-Server auf dem Access Point die DNS-Konfiguration. Dadurch konnten WLAN-Clients keine DNS-Auflösung durchführen und der Redirect auf den Hotspot funktionierte nicht.

→ Der DHCP-Server des LMC-Hotspots auf einem Access Point unterstützt nur IPv4. Fungierte der Access Point als Hotspot-Gateway und wurde diesem ein IPv6-DNS-Server zugewiesen, verwarf der DHCP-Server auf dem Access Point die DNS-Konfiguration. Dadurch konnten WLAN-Clients keine DNS-Auflösung durchführen und der Redirect auf den Hotspot funktionierte nicht.

→ Im Pfad ‚/Status/WLAN/Interfaces' blieb der Wert ‚Beacon-Rate' auf 6 MBit/s stehen, wenn ein anderer Wert eingestellt war, welcher mit einem Wert aus der Spalte ‚Supported Rates' übereinstimmte (z.B. 12 MBit/s).

→ In LCOS LX 6.20 Rel sendeten die Access Points im DHCP-Request den ‚Host Name' nicht mehr mit.

→ Eine per WEBconfig heruntergeladene Gerätekonfiguration, die nach dem Herunterladen verändert wurde, ließ sich nicht wieder per WEBconfig in das Gerät laden.

→ Wenn sich ein WLAN-Client mit einem Cloud-managed Hotspot mit externem Captive Portal verband, aber noch nicht authentifiziert war, konnte der Client das Internet ohne Einschränkungen über IPv6 nutzen, wenn der Access Point zusätzlich zum (aufgrund nicht vorhandener Authentifizierung) geblockten IPv4 auch über IPv6 verbunden war.

→ Bei Verwendung von TACACS+ erfolgt in der Standard-Konfiguration ein Fallback auf die lokalen Benutzer, wenn der TACACS+-Server nicht erreichbar ist. Der Fallback auf die lokalen Benutzer erfolgte aber auch dann, wenn der TACACS+-Server erreichbar war.

LCOS LX - Änderungen 6.20.0078 Rel

Neue Features

Allgemein

→ Unterstützung für das TACACS+-Protokoll
→ Diverse Verbesserungen im WEBconfig-Onboarding-Dialog
→ IEEE 802.3az / EEE ist nun konfgurierbar.
→ Für Digital Signage / ESL kann ein eigenes IP/VLAN-Interface konfiguriert werden.
→ Die SSH-Hostkey-Länge kann konfiguriert werden.
→ Das Message-Authenticator-Attribut kann nun in RADIUS-Nachrichten erzwungen werden.

WLAN

→ Aktualisierung des WLAN-Treibers für erhöhte Stabilität und Kompatibilität
→ Unterstützung des LANCOM Sustainability Mode / WLAN-Energiesparmodus mit der LANCOM Management Cloud
→ Die DTIM-Periode ist nun konfigurierbar.
→ Neue WLAN-Landeseinstellungen: Kanada, Liechtenstein
→ Die in Beacons angekündigten ‚Basic Rates' und ‚Supported Rates' sind nun konfigurierbar.
→ Eine zufällige WLAN-Kanalwahl ist konfigurierbar.
→ Ausrichtungs-Assistent für WLAN-Funkstrecken in der WEBconfig

LMC-Betrieb

→ Bei Verwendung des LMC-Hotspots wird der Anmeldestatus der Benutzer zwischen den einzelnen APs des Hotspots im LAN geteilt, um schnelleres Roaming zu ermöglichen.
→ Unterstützung für Frederix Hotspot

WLC-Betrieb

→ WLC-Skripte werden nun unterstützt.
→ Im WLC-Betrieb werden nun L2TPv3-Tunnel als Alternative zu WLC-L3-Tunneln unterstützt.
→ In Active-Active-Szenarien wird nun das Element AC-IPv4-List ausgewertet, um weitere WLCs des Active-Active-Clusters zu lernen.

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de | lancom-systems.de

Unicast zu senden. Dies konnte der LCOS LX Access Point nicht interpretieren und sendete keine Rückmeldung.

→ Wenn eine SSID mit LEPS-MAC konfiguriert wurde, für diese jedoch keine Verschlüsselung verwendet wurde, funktionierte die Blacklist bzw. Whitelist nicht.

→ Es wurde eine Sicherheitslücke in der UTF32Encoding.cpp der POCO-Bibliothek behoben (CVE-2023-52389).

→ Wenn ein LANCOM LX-6500(E) via PoE betrieben wurde und zu wenig Leistung erhielt (802.3at), wurde der zweite Port auf 100 MBit/s gedrosselt. In der Folge konnte das LACP nicht mehr funktionieren, da hier gleiche Port-Geschwindigkeiten benötigt werden. Das LACP wurde jedoch weiter als aktiv angezeigt, obwohl dies nicht der Fall war.

→ Wurde in einer SSID mit Dynamic-VLAN und in einer weiteren SSID die gleiche VLAN-ID verwendet, konnte die VLAN-ID per Dynamic-VLAN nicht zugewiesen werden. Dies führte dazu, dass in dieser SSID keine Kommunikation möglich war.

→ Wenn in einer SSH-Konsolen-Sitzung im Pfad ‚Setup/WLAN/Rate-Selection' der Befehl ‚set <Profilname> ?' eingegeben wurde (z.B. ‚set Network-Name ?'), beendete dies die Sitzung.

→ In der Detailkonfiguration der LMC war es nicht erlaubt, ein ‚#' in der LEPS-WPA-Passphrase zu verwenden, obwohl dies in LCOS LX erlaubt ist.

→ Wurden mehrere zusätzliche VLANs in einer WDS-Verbindung hinzugefügt, verlor die Verbindung anschließend die VLAN-Konfiguration. Dadurch war die Kommunikation über die WDS-Verbindung nur noch stark eingeschränkt oder gar nicht mehr möglich.

→ Es war nicht möglich, im Konsolen-Pfad ‚Setup/LMC' den Wert ‚Only-Without-WLC' zu setzen.

→ Es wurde eine Sicherheitslücke im wpa_supplicant behoben (CVE-2023-52160).

→ Der Antennengewinn konnte lediglich zwischen 0 und 15 dBi eingestellt werden. Dies wurde auf 0 bis max. 30 dBi geändert.

→ Bei WLAN-Clients, die mit einem Netzwerk mit statisch zugewiesener VLAN-ID verbunden waren, wurde die VLAN-ID nicht in der Tabelle ‚Status/WLAN/Station-Table' angezeigt.

→ Im Pfad ‚Status/WLAN/Channels-Allowed-By-Regulator' fehlten die erlaubten 6 GHz-Kanäle für die Länder Bulgarien und Ungarn.

→ Beim Auslesen einer SNMPv2-MIB wurden im Pfad ‚Setup/Config/Location' die Informationen für Location und Administratorname nicht ausgelesen und in die

7. Allgemeine Hinweise

Haftungsausschluss

Die LANCOM Systems GmbH übernimmt keine Gewähr und Haftung für nicht von der LANCOM Systems GmbH entwickelte, hergestellte oder unter dem Namen der LANCOM Systems GmbH vertriebene Software, insbesondere nicht für Shareware und sonstige Fremdsoftware.

Sichern der aktuellen Konfiguration

Bitte sichern Sie vor dem Update Ihrer LANCOM Geräte auf eine neue LCOS LX -Version unbedingt Ihre Konfigurationsdateien!

Wegen umfangreicher Feature-Erweiterungen ist ohne eine Sicherung der Konfigurationsdaten eine Rückkehr auf eine ältere Firmware **nicht mehr automatisch möglich.**

Wir empfehlen zudem, dass produktive Systeme vor dem Einsatz in der Kundenumgebung erst einem internen Test unterzogen werden, da trotz intensivster interner und externer Qualitätssicherungsmaßnahmen ggf. nicht alle Risiken durch LANCOM Systems ausgeschlossen werden können.

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de | lancom-systems.de